UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,020	01/17/2001	Travis Kelly Harper	15267.3	8056

7590 08/05/2004

John M. Guynn
WORKMAN, NYDEGGER & SEELEY
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	3

DATE MAILED: 08/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/764,020	**Applicant(s)** HARPER ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

1. Pursuant to USC 131, claims 1-39 are presented for examination.

Specification

2. The disclosure is objected to because of the following informalities: there is inconsistency on page 30, on the description of element 160 described as "phone line" and "secure channel" and element 162 described as both courier service and ordinary mail.

Applicant is requested to carefully review the application to correct any similar errors.

2.1 The abstract of the disclosure is objected to because of the "means" expression on line 13. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Objections

3. **Claim 15** is objected to because of the following informalities: "A method as defined in claim 15" needs to be corrected to avoid rendering the claim indefinite. Appropriate correction is required.

Claim 11 is objected to because of the following informalities: in order to avoid rendering the claim indefinite, the term “capable of” should be corrected. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4.1 Regarding **claim 24** the phrase "a computer-readable medium at least partially separate from the computer readable medium of claim 23" renders the claim indefinite because the claim includes elements not actually disclosed (those encompassed by " at least partially separate "), thereby rendering the scope of the claim unascertainable.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 1-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,799,088 to **Raike** in view of Bruce Schneier; Applied Cryptography; 1996 by John Wiley & Sons; Second Edition; Pages 311-313.

5.2 **As per claims 1, 13, 22-24, Raike** substantially teaches a method and system for protecting an electronic file from unauthorized access, copying or alteration, comprising: (a) providing a plaintext file that includes blocks of original binary data to be encrypted, said blocks having a given length and a maximum possible integer value, for example (see column 15, lines 15-55); (b) providing a key K that meets the recitation of first key that includes a number of indexed integer values selected from a set bounded below by 0 or 1 and above by the maximum possible integer value of the blocks of binary data to be encrypted, for example (see column 14, line 45 through column 15, line 10); (c) providing R or D that meets the recitation of second key that includes a number of indexed integer values selected from a set bounded below by 0 and above by the predetermined number of indexed integer values included in the first key, for example (see column 14, lines 7-45); (d) providing a key algorithm that relates the first and second keys together, for example (see column 14, lines 45-55); (e) selecting from the plaintext file a block of binary data to be encrypted, for example (see column 15, lines 15-55); (f) **Raike** discloses using value from the second key into the first key to generate one or more values of K that meets the recitation of selecting, according to the key algorithm, an integer value from the second key and (g) inputting, according to the key algorithm, the integer value selected from the second key into the first key so as to obtain one or more integer values, for example (see column 14, lines 28-67); (h) performing an XOR process on the block of original binary data using the one or more integer values obtained from the first key so as to generate a block of encrypted binary data, for example (see column 15, lines 1-15); and (i) repeating steps (e)-(h) until a desired portion the plaintext file has been encrypted so as to yield a ciphertext file including blocks of encrypted binary data, for example (see column 15, lines 3-40). It is apparent to one skilled in the art that the disclosure of **Raike** meets the recitation of the limitations of claim 1. Minor variations can be performed by one skilled in the art as **Raike** mentions. **Schneier** in an analogous art teaches a block algorithm with use of masks as one of the unique features wherein numbers are derived from the key table that are used to select the tables in a given function within a given round. Both the value of the data and the masks are used together to select the function tables, which provides security against attacks, for example (see pages 311-313). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Raike** to provide the option of selecting, according to the key algorithm, an integer value from the second key and (g) inputting, according to the key algorithm, the integer value selected from the second key into the first key so as to obtain one or more integer values as taught by **Schneier**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Schneier** so as to provide additional security against attacks.

As per claims 2-6, Raike discloses the limitation of size variation of the plaintext and key data to be encrypted that meets the recitation of wherein the blocks of original binary data to be encrypted are one byte in length and have a maximum numeric value of 255 and wherein the integer values included in the first key are selected from a set bounded below by 0 or 1 and bounded above by 255, and wherein the integer values contained in the first key and the second key are random or pseudo-random numbers, for example (see column 17, lines 1-67; column 15, lines 15-55 and column 14). **Raike** also discloses variation in key length modulo operation etc. that meets the recitation of wherein the number of integer values obtained from the first key and used in encrypting the block of original binary data is determined by a remainder value generated by dividing the integer value selected from the second key by a predetermined divisor, wherein the number of integer values within the first key is 2048, wherein the number of integer values within the second key is 2048, and wherein the predetermined divisor used to generate the remainder value is 20, for example (see column 18, lines 1-42). It is apparent that one skilled in the art can use any mathematical algorithm for the size and selection of keys and integer values without departing from the spirit and scope of the invention disclosed by **Raike**.

As per claim 7, Raike discloses the limitation of wherein the first integer value selected from the second key when encrypting the first block of original binary data is selected from index position 0, for example (see column 16, lines 21-67 and column 18, lines 1-42) and discloses selecting index position using mathematical algorithm. Such technique is known in the art as it is disclosed for example in US Patent 5,131,039. **Raike** further discloses imposing restriction or condition on byte position selection, for example (see column 17, lines 49-67 and column 23, lines 9-35). Therefore, it would have been obvious to one skilled in the art to modify the algorithm of **Raike** to update each immediately preceding index position by the value of the immediately preceding block of encrypted binary data and then selecting the integer value contained in the updated index position, provided when a number exceeds the highest possible index position the index position is reset to 0. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Raike** so as to achieve different security objective, for example (see column 15, lines 24-65 and column 23, lines 9-67).

As per claim 8, Raike discloses the limitation of wherein the XOR process is modified so that it is not commutative, for example (see column 15, lines 24-45).

As per claims 9-10, Raike discloses the limitation of further including the step of storing the ciphertext file together with the first key so as to yield an encrypted file wherein the encrypted file is stored in a manner so as to have a unique suffix appended to the name of the encrypted file and thereby identify the encrypted file as being of a unique file type, for example (see column 16, lines 3-9 and column 14, lines 19-45; and column 17, line 63 through column 18, line 10).

As per claim 11, Raike discloses the limitation of further including the steps of sending to a decrypting party the encrypted file of the unique file type and providing the decrypting party with software capable of decrypting the encrypted file, so as to yield at least a portion of the plaintext file and outputting data corresponding to information contained within the plaintext file, for example (see column 18, line 40 through column 19, line 3; see also column 19-20 for decryption details).

As per claim 12, Raike discloses the limitation of wherein the software limits or prevents copying alteration or sending of the information contained within the plaintext file by the decrypting party, for example (see column 17, line 63 through column 18, line 10 and column 21, lines 1-10).

As per claims 14-15, Raike discloses the limitation of wherein the ciphertext and first key are provided to the decrypting party by means of a transmission by an encrypting party over the Intemet, for example (see column 31, lines 30-47). Secure transfer through the Internet using HTTPS is well known in the art.

As per claims 16-17, Raike discloses the limitation of using secure storage for distribution of key and key algorithm, and also discloses using secure transfer for secure data and authorization data and the use of password to retrieve keys that meets the limitations of and wherein the second key and key algorithm are provided to the decrypting party as part of a computer-readable medium, wherein the second key is provided to the decrypting party by means of a password protected login procedure over a secure line between the decrypting party and an encrypting party, for example (see column 31, lines 2-67).

As per claims 18-20, Raike discloses the limitation of performing file encryption and also discloses that the invention can be implemented in voice data and further discloses generating keys from a drawing pattern, for example (see column 31, lines 2-67). . It is obvious that the invention can be implemented with a graphic file or any file format known in the art, for example (see US Patent 6,011,849).

As per claims 21, 25, Raike discloses the limitation of using a unique key to the plaintext file, for example (see column 21, lines 45-63 and column 22, line 25-30 and (see column 16, lines 3-9 and column 14, lines 19-45; and column 17, line 63 through column 18, line 10).

6. **Claims 26-39** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,799,088 to **Raike** in view of US Patent US Patent 5,809,145 to **Slik et al.**.

6.1 **As per claims 26 and 32, Raike** substantially teaches a method and system for protecting an electronic file sent over the Internet from unauthorized access, copying or alteration, comprising: (a) encrypting a plaintext file using an encryption algorithm, a public key, and a private key so as to generate a ciphertext file, for example (see column 14); (b) storing the ciphertext file together with the public key so as to yield a composite file of a unique file type, for example (see column 16, lines 3-9 and column 14, lines 19-45; and column 17, line 63 through column 18, line 10); (c) sending the composite file to an authorized decrypting party over the Internet, for example (see , for example (see column 31, lines 30-47); **Raike** discloses generating the private key and discloses providing algorithm together with the public key provided as part of the composite file, allow the decrypting party to at least partially decrypt the ciphertext file and restore at least a portion of the plaintext file, for example (see column 14, lines 21-55). **Slik et al.** in an analogous art teaches (d) separately providing the decrypting party with the private key and a decryption algorithm corresponding to the encryption algorithm which, together with the public key provided as part of the composite file, allow the decrypting party to at least partially decrypt the ciphertext file and restore at least a portion of the plaintext file, for example (see column 17, line 35 through column 18, line 57) with of the many advantages to prevent the unlocking of datasets on unauthorized computers, for example (see column 3, paragraphs 50-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Raike** to separately provide the decrypting party with the private key and a decryption algorithm as taught by **Slik et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Slik et al.** so as to prevent the unlocking of datasets on unauthorized computers.

As per claims 27-28, 29-31, 34, and 35, Slik et al. in an analogous art teaches wherein the private key and decryption algorithm are integrated together as part of a restricted output algorithm which inhibits or prevents copying, alteration and sending of the restored portion of the plaintext file, wherein the plaintext file digitally represents information contained in a tangible document and wherein the restricted output algorithm includes an algorithm for outputting at least a portion of the information contained in the tangible document to allow customers to preview before purchasing and to verify that the customer is permitted to have access to the data, for example (see column 7, line 31 through column 8, line 39). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Raike** to provide the limitation wherein the private key and decryption algorithm are integrated together as part of a restricted output algorithm which inhibits or prevents copying, alteration and sending of the restored portion of the plaintext file as taught by **Slik et al.** This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Slik et al.** in order to allow customers to preview before purchasing and to verify that the customer is permitted to have access to the data, for example (see column 7, line 31 through column 8, line 39).

Claims 33 and 39 recite some of the limitation found in claims 26-27. Therefore, **claims 33 and 39** are rejected on the same rationale as the rejection of claims 26-27.

Claims 36-38 recite the same limitations as claims 17 and 21. Therefore, **claims 36-38** are rejected on the same rationale as the rejection of claims 17 and 21.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses the use of protecting electronic file from unauthorized access.

US Patent:	6,011,849	Orrin

US Patent Publication	US 2002/0184485	Dray JR. et al.

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

ce

Carl Colin

Patent Examiner

July 26, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100